DEFENSE INFORMATION SYSTEMS AGENCY
P. O. BOX 4502
ARLINGTON, VIRGINIA 22204-4502

IN REPLY REFER TO: Joint Interoperability Test Command (JTE) **30 Dec 10**

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Special Interoperability Test Certification of the L-3 Communications Internet Protocol (IP) Secure Terminal Equipment (STE) Version 1.2.4

References:
(a) DoD Directive 4630.05, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," 5 May 2004
(b) CJCSI 6212.01E, "Interoperability and Supportability of Information Technology and National Security Systems," 15 December 2008
(c) through (h), see Enclosure 1

1. References (a) and (b) establish the Defense Information Systems Agency (DISA), Joint Interoperability Test Command (JITC), as the responsible organization for interoperability test certification.

2. The L-3 Communications IP STE Version 1.2.4 is hereinafter referred to as the system under test (SUT). The SUT meets all of its critical interoperability requirements and is certified for joint use within the Defense Information System Network (DISN) as a Department of Defense (DoD) Secure Communications Device (DSCD). The SUT is certified with any Cisco CallManager (CCM) solution on the Unified Capabilities (UC) Approved Product List (APL) or Cisco Unified Communications Manager (CUCM) with software version 7.1(2) with the following limitation: the CCM solution must be configured with 2800, 3700, or 3800 series gateways that are loaded with Internetwork Operating System (IOS) versions 12.4(22)T2 or later for the 2800 series gateways and IOS 12.4(15) T8 or later for the 3700 and 3800 series gateways. No other configurations, features, or functions, except those cited within this report, are certified by the JITC. This certification expires upon changes that could affect interoperability, but no later than three years from the date of Defense Information Assurance (IA)/Security Accreditation Working Group (DSAWG) accreditation.

3. This finding is based on interoperability testing conducted by JITC, review of the vendor's Letters of Compliance (LoC), adjudication of open test discrepancy reports by DISA and Theater Joint Tactical Network (TJTN), waiver of Internet Protocol version 6 (IPv6) requirements, National Security Agency (NSA) Type I Accreditation, and DSAWG accreditation. Interoperability testing of the SUT was conducted at JITC's Global Information Grid Network Test Facility at Fort Huachuca, Arizona, from 8 March through 30 April 2010. Review of vendor's LoC was completed on 4 May 2010. The DISA and TJTN adjudication of outstanding test discrepancy reports was completed on 23 April 2010. The Office of the Secretary of Defense waived the IPv6 requirements on 27 September 2010 with the stipulation that the vendor

provide a commitment to upgrade to IPv6 and demonstrate it during the Spiral 2 IPv6 Pilot test starting in the summer of 2011. The SUT NSA Type I accreditation was granted on 12 October 2010, References (c) and (d). The DSAWG granted accreditation on 23 November 2010 based on the security testing completed by DISA-led IA test teams and published in a separate report, Reference (e). Enclosure 2 documents the test results and describes the tested network and system configurations.

4. The interoperability test summary of the SUT is indicated in Table 1. The Unified Capabilities Requirement DSCD Interoperability Requirements are listed in Table 2. This interoperability test status is based on the SUT's ability to meet:

a. Defense Switched Network (DSN) services for Network and Applications specified in Reference (f).

b. DSCD interface and signaling requirements as specified in Reference (g) verified through JITC testing and/or vendor submission of LoC.

c. DSCD Capability Requirements (CRs)/Feature Requirements (FRs) specified in Reference (g) verified through JITC testing and/or vendor submission of LoC.

d. The overall system interoperability performance derived from test procedures listed in Reference (h).

Table 1. SUT Interoperability Test Summary

DSCD Interoperability Requirements			
Interface & Signaling	**Critical**	**Status**	**Remarks**
Ethernet 100BaseT (SCCP) (IEEE 802.3u)	Yes	Certified	When testing the IP STE with CUCM software version 8.0.2, calls were unable to be placed from the SUT. Therefore the SUT is not certified with any release of the CUCM after 7.1(2).[1] The SUT met all Critical CRs and FRs with the following minor exceptions: The one-way latency was measures at 65 ms.[2] The SUT does not support IPv6.[3] The SUT does not set DSCP for any value 0 to 63.[4]
Security	Yes	Certified	See note 5.

NOTES:

1 The SUT is certified with any CCM solution on the UC APL or CUCM with software version 7.1(2) with the following limitation with the following limitation: the CCM solution must be configured with 2800, 3700, or 3800 series gateways that are loaded with IOS versions 12.4(22)T2 or later for the 2800 series gateways and IOS 12.4(15) T8 or later for the 3700 and 3800 series gateways.

2 The SUT had a measured one-way latency of 65 ms from handset to the T1 ISDN PRI gateway trunk egress, which did not meet this requirement. This discrepancy was adjudicated by DISA and the TJTN as having a minor operational impact.

3 The Office of the Secretary of Defense waived the IPv6 requirements on 27 September 2010 with the stipulation that the vendor provide a commitment to upgrade to IPv6 and demonstrate it during the Spiral 2 IPv6 Pilot test starting in the summer of 2011.

4 The SUT is hard coded with DSCP values of 0 for signaling and 40 for media. This discrepancy was adjudicated by DISA and the TJTN as having a minor operational impact with a POAM. The vendor stated in their POAM that this capability will be added in the next release of the SCCP IP STE in late 2011.

5 Security is tested by DISA-led Information Assurance test teams and published in a separate report, Reference (d).

Table 1. SUT Interoperability Test Summary (continued)

LEGEND:

802.3u	Standard for carrier sense multiple access with collision detection at 100 Mbps
APL	Approved Products List
CCM	Cisco CallManager
CRs	Capability Requirements
CUCM	Cisco Unified Communications Manager
DISA	Defense Information Systems Agency
DSCD	Department of Defense (DoD) Secure Communications Device
DSCP	Differentiated Services Code Point
FRs	Feature Requirements
IEEE	Institute of Electrical and Electronics Engineers
IOS	Internetwork Operating System
IP	Internet Protocol
IPv6	Internet Protocol version 6
ISDN	Integrated Services Digital Network
Mbps	Megabits per second
POAM	Plan of Action and Milestones
PRI	Primary Rate Interface
SCCP	Skinny Client Control Protocol
STE	Secure Terminal Equipment
SUT	System Under Test
T1	Digital Transmission Link Level 1 (1.544 Mbps)
TJTN	Theater Joint Tactical Network
UC	Unified Capabilities

Table 2. DSCD UCR Interoperability Requirements

DSN Line Interface			
Interface	**Critical**	**Requirements Required or Conditional**	**References**
Ethernet 100BaseT (SCCP)	Yes	• Type Approved by NSA (R) • DSCDs that establish secure sessions on IP networks using FNBDT/SCIP shall satisfy all of the end point requirements described SCIP-215 and SCIP-216 (C) • DSCD devices that use an IP interface shall meet the end instrument requirements as specified in UCR 2008 Change 1, Section, 5.3.2 (C) • Shall go secure with at least an 85% call completion rate (R) • Shall establish secure call within 60 seconds for duration of secure call (R) • Shall operate in a network that has an end-to-end latency of up to 600 milliseconds (R) • Maintain secure voice connection with MOS of 3.0 (R) • Process new key with 95% rekey completion rate (R) • Supports data and facsimile transmission rate of 9.6 kbps or better (C)	• UCR Section 5.2.5.2 • UCR Section 5.2.5.2 • UCR Section 5.2.5.2 • UCR Section 5.2.5.2 • UCR Section 5.2.5.2 • UCR Section 5.2.5.2 • UCR Section 5.2.5.2 • UCR Section 5.2.5.2 • UCR Section 5.2.5.2
Security		• GR-815, STIGs, and DoDI 8510.bb (DIACAP) (R)	• UCR Section 3

LEGEND:

100BaseT	100 Mbps (Baseband Operation, Twisted Pair) Ethernet
C	Conditional
DIACAP	DoD Information Assurance Certification and Accreditation Process
DoD	Department of Defense
DoDI	DoD Instruction
DSCD	DoD Secure Communications Device
DSN	Defense Switched Network
FNBDT	Future Narrowband Digital Terminal
GR	Generic Requirement
GR-815	Generic Requirements For Network Element/Network System (NE/NS) Security
IP	Internet Protocol
kbps	kilobits per second
Mbps	Megabits per second
MOS	Mean Opinion Score
NSA	National Security Agency
R	Required
SCCP	Skinny Client Control Protocol
SCIP	Secure Communications Internet Protocol
STIGs	Security Technical Implementation Guides
UCR	Unified Capabilities Requirements

5. No detailed test report was developed in accordance with the Program Manager's request. JITC distributes interoperability information via the JITC Electronic Report Distribution (ERD) system, which uses Unclassified-But-Sensitive Internet Protocol Router Network (NIPRNet) e-mail. More comprehensive interoperability status information is available via the JITC System Tracking Program (STP). The STP is accessible by .mil/gov users on the NIPRNet at https://stp.fhu.disa.mil. Test reports, lessons learned, and related testing documents and references are on the JITC Joint Interoperability Tool (JIT) at http://jit.fhu.disa.mil (NIPRNet), or http://199.208.204.125 (SIPRNet). Information related to DSN testing is on the Telecom Switched Services Interoperability (TSSI) website at http://jitc.fhu.disa.mil/tssi. Due to the

sensitivity of the information, the Information Assurance Accreditation Package (IAAP) that contains the approved configuration and deployment guide must be requested directly through government civilian or uniformed military personnel from the Unified Capabilities Certification Office (UCCO), e-mail: ucco@disa.mil.

6. The JITC point of contact is Mr. Joseph Roby, DSN 879-0507, commercial (520) 538-0507, FAX DSN 879-4347, or e-mail to joseph.roby@disa.mil. The JITC's mailing address is P.O. Box 12798, Fort Huachuca, AZ 85670-2798. The tracking number for the SUT is 0920506.

FOR THE COMMANDER:

Steve Lasneski

2 Enclosures a/s

for RICHARD A. MEADOR
Chief
Battlespace Communications Portfolio

Distribution (electronic mail):
Joint Staff J-6
Joint Interoperability Test Command, Liaison, TE3/JT1
Office of Chief of Naval Operations, CNO N6F2
Headquarters U.S. Air Force, Office of Warfighting Integration & CIO, AF/XCIN (A6N)
Department of the Army, Office of the Secretary of the Army, DA-OSA CIO/G-6 ASA (ALT), SAIS-IOQ
U.S. Marine Corps MARCORSYSCOM, SIAT, MJI Division I
DOT&E, Net-Centric Systems and Naval Warfare
U.S. Coast Guard, CG-64
Defense Intelligence Agency
National Security Agency, DT
Defense Information Systems Agency, TEMC
Office of Assistant Secretary of Defense (NII)/DOD CIO
U.S. Joint Forces Command, Net-Centric Integration, Communication, and Capabilities Division, J68
Defense Information Systems Agency, GS23

ADDITIONAL REFERENCES

(c) National Security Agency, "Information Assurance Directorate Certificate," 21 September 2007

(d) National Security Agency Secure Terminal Equipment (STE) Program Office, "Engineering Change Proposal," 12 October 2010

(e) Joint Interoperability Test Command, "Information Assurance (IA) Assessment of L-3 Communications Internet Protocol (IP) Secure Terminal Equipment (STE) Release (Rel.) 1.2.4 (Tracking Number 0922205)," 23 November 2010

(f) Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6215.01C, "Policy for Department of Defense Voice Services with Real Time Services (RTS)," 9 November 2007

(g) Office of the Assistant Secretary of Defense, "Department of Defense Unified Capabilities Requirements 2008 Change 1," 22 January 2010

(h) Joint Interoperability Test Command, "Defense Switched Network Generic Switch Test Plan (GSTP), Change 2," 2 October 2006

CERTIFICATION TESTING SUMMARY

1. SYSTEM TITLE. L-3 Communications Internet Protocol (IP) Secure Terminal Equipment (STE) Version 1.2.4; hereinafter referred to as the System Under Test (SUT).

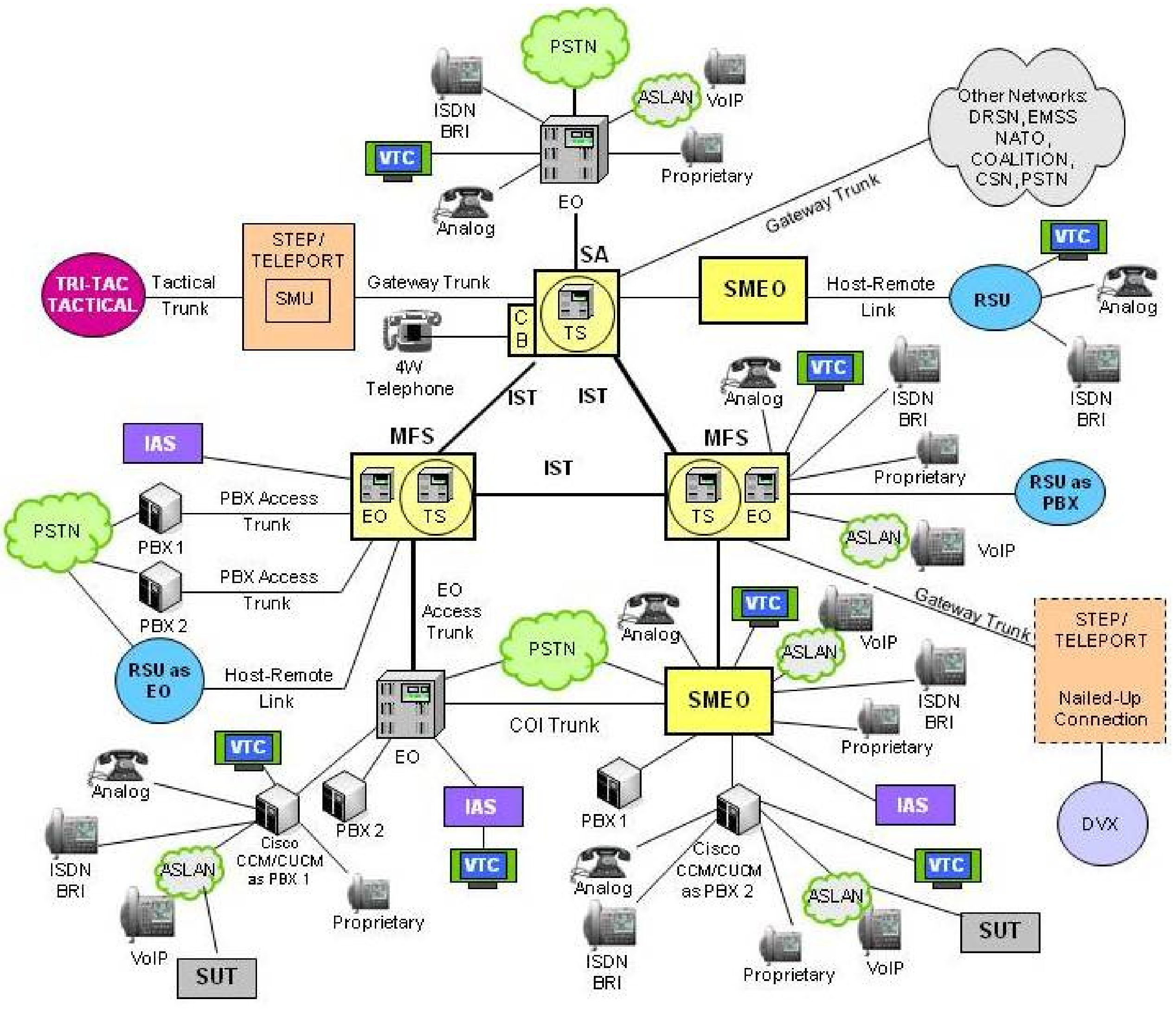
2. PROPONENT. U.S. Army Communications-Electronics Command.

3. PROGRAM MANAGER. Mr. John Kahler, EA-TJTN/GS13, Building 1210 Rittko Avenue, Fort Monmouth, New Jersey, 07703, E-mail: john.kahler@us.army.mil.

4. TESTER. Joint Interoperability Test Command (JITC), Fort Huachuca, Arizona.

5. SYSTEM UNDER TEST DESCRIPTION. The SUT is a Department of Defense (DoD) Secure Communications Device (DSCD) that provides voice communications for both secure (National Security Agency [NSA] Accredited Type 1) and non secure communications between other Cisco proprietary Voice over Internet Protocol (VoIP) users and Time Division Multiplex DSCD and non-DSCD end instruments which incorporate Secure Communication Internet Protocol (SCIP) technology. The SUT is an Internet Protocol (IP) end instrument and is only capable of being configured for use on the Cisco CallManager (CCM) or Cisco Unified Communications Manager (CUCM). The SUT is certified with any CCM solution on the Unified Capabilities (UC) Approved Product List (APL) or CUCM with software version 7.1(2) with the following limitation: the CCM solution must be configured with 2800, 3700, or 3800 series gateways that are loaded with Internetwork Operating System (IOS) versions 12.4(22)T2 or later for the 2800 series gateways and IOS 12.4(15) T8 or later for the 3700 and 3800 series gateways.

6. OPERATIONAL ARCHITECTURE. The Defense Switched Network (DSN) architecture is a two-level network hierarchy consisting of DSN backbone switches and Service/Agency installation switches. Joint Staff policy and subscriber mission requirements determine which type of switch can be used at a particular location. The DSN architecture, therefore, consists of several categories of switches, including Private Branch Exchanges (PBX)s. The Unified Capabilities Requirements (UCR) operational DSN Architecture is depicted in Figure 2-1.



LEGEND:

ASLAN	Assured Services Local Area Network
4W	4-Wire
BRI	Basic Rate Interface
CB	Channel Bank
CCM	Cisco CallManager
COI	Community of Interest
CSN	Canadian Switch Network
CUCM	Cisco Unified Communications Manager
DRSN	Defense Red Switch Network
DSN	Defense Switched Network
DVX	Deployable Voice Exchange
EMSS	Enhanced Mobile Satellite System
EO	End Office
IAS	Integrated Access Switch
ISDN	Integrated Services Digital Network
IST	Interswitch Trunk
MFS	Multifunction Switch
NATO	North Atlantic Treaty Organization
PBX	Private Branch Exchange
PBX 1	Private Branch Exchange 1
PBX 2	Private Branch Exchange 2
PSTN	Public Switched Telephone Network
RSU	Remote Switching Unit
SMEO	Small End Office
SMU	Switched Multiplex Unit
STEP	Standardized Tactical Entry Point
TDM/P	Time Division Multiplex/Packetized
Tri-Tac	Tri-Service Tactical Communications Program
TS	Tandem Switch
VoIP	Voice over Internet Protocol
VTC	Video Teleconferencing

Figure 2-1. DSN Architecture

7. REQUIRED SYSTEM INTERFACES. The SUT Interoperability Test Summary is shown in Table 2-1 and the Capability and Feature Requirements used to evaluate the interoperability of the SUT are indicated in Table 2-2. These requirements are derived from the UCR and verified through JITC testing and review of the vendor's Letters of Compliance (LoC).

Table 2-1. SUT Interoperability Test Summary

DSCD Interoperability Requirements			
Interface & Signaling	**Critical**	**Status**	**Remarks**
Ethernet 100BaseT (SCCP) (IEEE 802.3u)	Yes	Certified	When testing the IP STE with CUCM software version 8.0.2, calls were unable to be placed from the SUT. Therefore the SUT is not certified with any release of the CUCM after 7.1(2).[1] The SUT met all Critical CRs and FRs with the following minor exceptions: The one-way latency was measures at 65 ms.[2] The SUT does not support IPv6.[3] The SUT does not set DSCP for any value 0 to 63.[4]
Security	Yes	Certified	See note 5.

NOTES:

1 The SUT is certified with any CCM solution on the UC APL or CUCM with software version 7.1(2) with the following limitation with the following limitation: the CCM solution must be configured with 2800, 3700, or 3800 series gateways that are loaded with IOS versions 12.4(22)T2 or later for the 2800 series gateways and IOS 12.4(15) T8 or later for the 3700 and 3800 series gateways.

2 The SUT had a measured one-way latency of 65 ms from handset to the T1 ISDN PRI gateway trunk egress, which did not meet this requirement. This discrepancy was adjudicated by DISA and the TJTN as having a minor operational impact.

3 The Office of the Secretary of Defense waived the IPv6 requirements on 27 September 2010 with the stipulation that the vendor provide a commitment to upgrade to IPv6 and demonstrate it during the Spiral 2 IPv6 Pilot test starting in the summer of 2011.

4 The SUT is hard coded with DSCP values of 0 for signaling and 40 for media. This discrepancy was adjudicated by DISA and the TJTN as having a minor operational impact with a POAM. The vendor stated in their POAM that this capability will be added in the next release of the SCCP IP STE in late 2011.

5 Security is tested by DISA-led Information Assurance test teams and published in a separate report, Reference (d).

LEGEND:

802.3u	Standard for carrier sense multiple access with collision detection at 100 Mbps
APL	Approved Products List
CCM	Cisco CallManager
CRs	Capability Requirements
CUCM	Cisco Unified Communications Manager
DISA	Defense Information Systems Agency
DSCD	Department of Defense (DoD) Secure Communications Device
DSCP	Differentiated Services Code Point
FRs	Feature Requirements
IEEE	Institute of Electrical and Electronics Engineers
IOS	Internetwork Operating System
IP	Internet Protocol
IPv6	Internet Protocol version 6
ISDN	Integrated Services Digital Network
Mbps	Megabits per second
POAM	Plan of Action and Milestones
PRI	Primary Rate Interface
SCCP	Skinny Client Control Protocol
STE	Secure Terminal Equipment
SUT	System Under Test
T1	Digital Transmission Link Level 1 (1.544 Mbps)
TJTN	Theater Joint Tactical Network
UC	Unified Capabilities

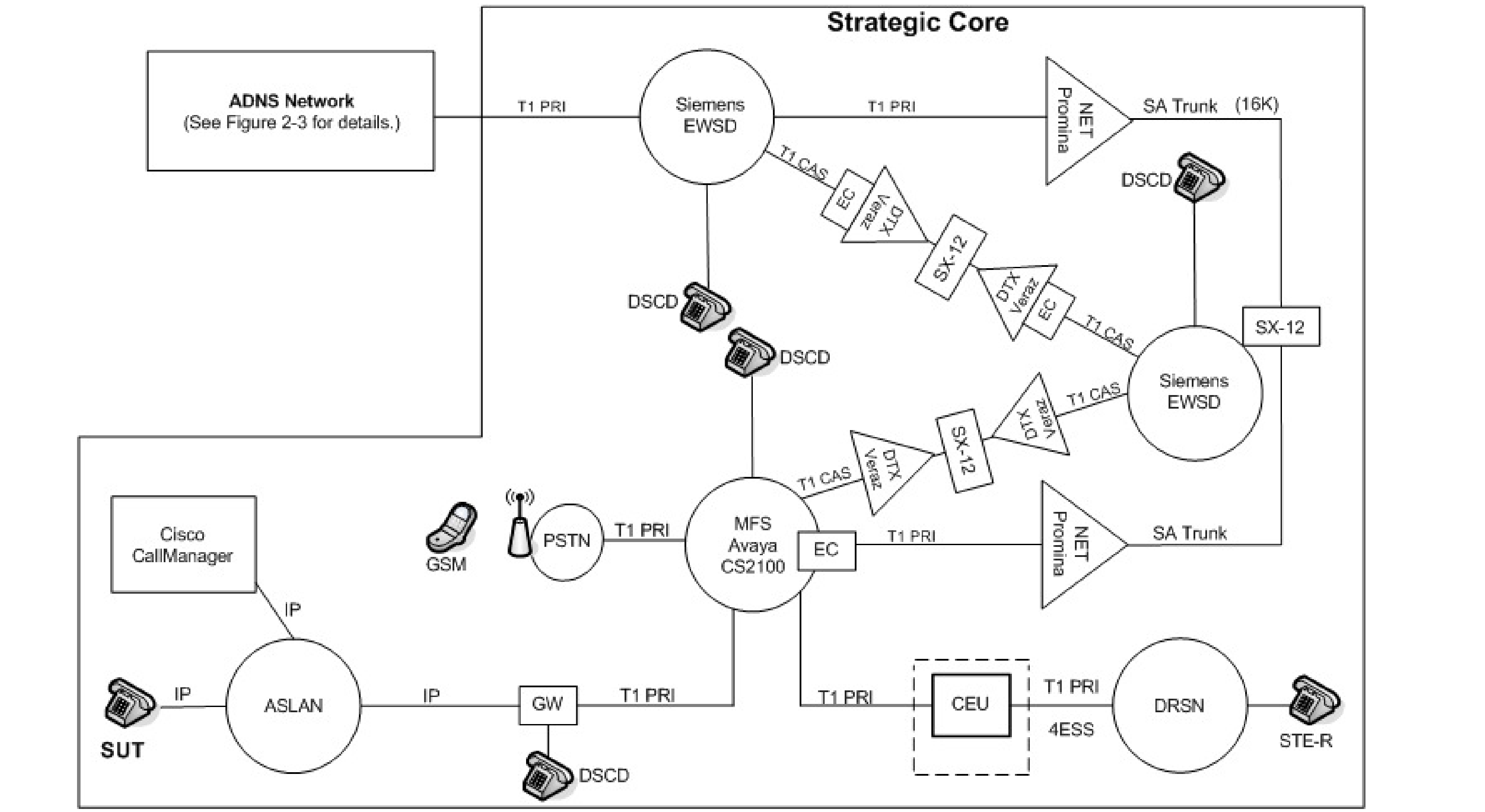
Table 2-2. DSCD UCR Interoperability Requirements

DSN Line Interface			
Interface	**Critical**	**Requirements Required or Conditional**	**References**
Ethernet 100BaseT (SCCP)	Yes	• Type Approved by NSA (R) • DSCDs that establish secure sessions on IP networks using FNBDT/SCIP shall satisfy all of the end point requirements described SCIP-215 and SCIP-216 (C) • DSCD devices that use an IP interface shall meet the end instrument requirements as specified in UCR 2008 Change 1, Section, 5.3.2 (C) • Shall go secure with at least an 85% call completion rate (R) • Shall establish secure call within 60 seconds for duration of secure call (R) • Shall operate in a network that has an end-to-end latency of up to 600 milliseconds (R) • Maintain secure voice connection with MOS of 3.0 (R) • Process new key with 95% rekey completion rate (R) • Supports data and facsimile transmission rate of 9.6 kbps or better (C)	• UCR Section 5.2.5.2 • UCR Section 5.2.5.2 • UCR Section 5.2.5.2 • UCR Section 5.2.5.2 • UCR Section 5.2.5.2 • UCR Section 5.2.5.2 • UCR Section 5.2.5.2 • UCR Section 5.2.5.2 • UCR Section 5.2.5.2
Security		• GR-815, STIGs, and DoDI 8510.bb (DIACAP) (R)	• UCR Section 3

LEGEND:

100BaseT	100 Mbps (Baseband Operation, Twisted Pair) Ethernet
C	Conditional
DIACAP	DoD Information Assurance Certification and Accreditation Process
DoD	Department of Defense
DoDI	DoD Instruction
DSCD	DoD Secure Communications Device
DSN	Defense Switched Network
FNBDT	Future Narrowband Digital Terminal
GR	Generic Requirement
GR-815	Generic Requirements For Network Element/Network System (NE/NS) Security
IP	Internet Protocol
kbps	kilobits per second
Mbps	Megabits per second
MOS	Mean Opinion Score
NSA	National Security Agency
R	Required
SCCP	Skinny Client Control Protocol
SCIP	Secure Communications Internet Protocol
STIGs	Security Technical Implementation Guides
UCR	Unified Capabilities Requirements

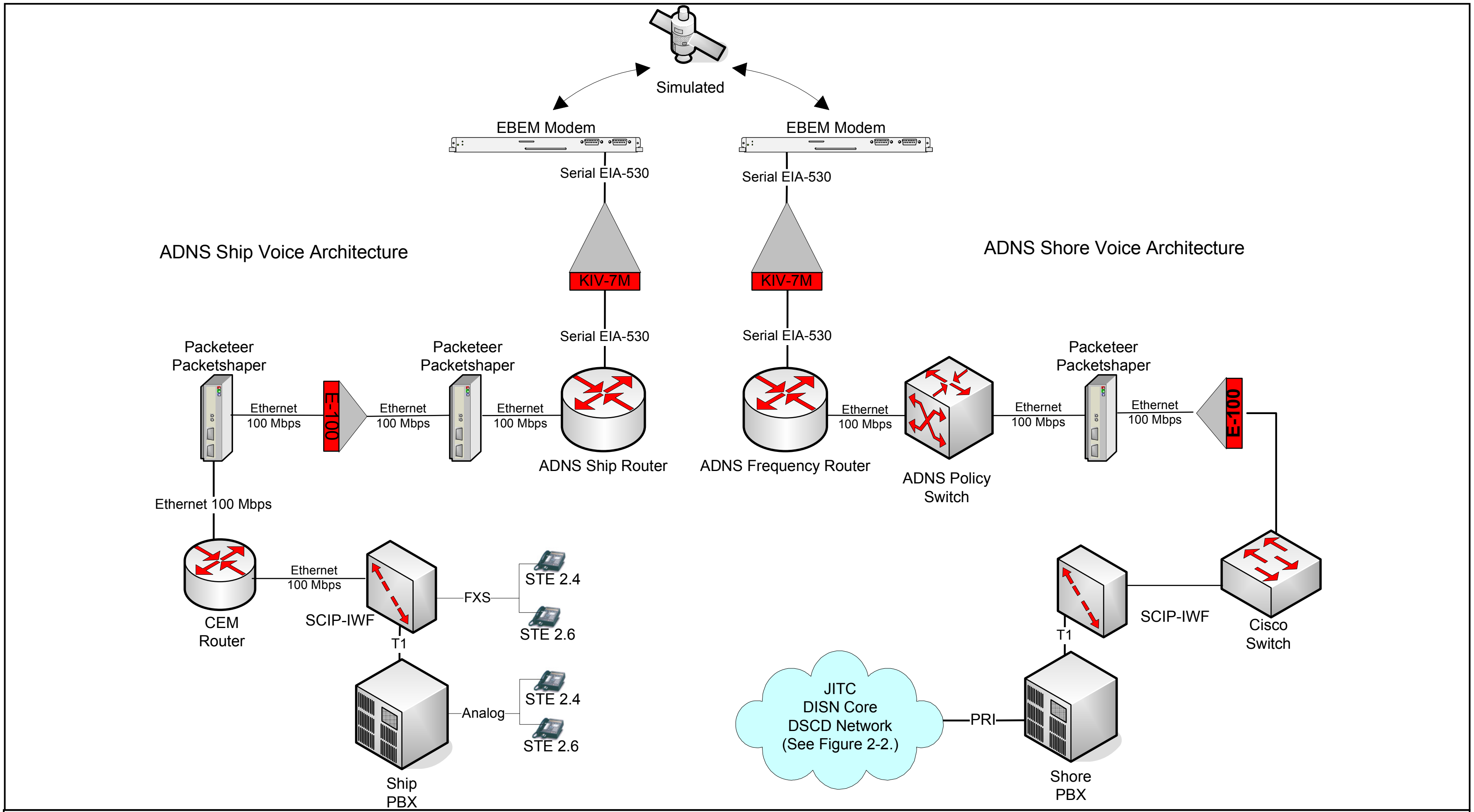
8. TEST NETWORK DESCRIPTION. The SUT was tested at JITC's Global Information Grid Network Test Facility in a manner and configuration similar to that of the DSN operational environment. Testing of the SUT required functions and features was conducted using the test configurations depicted in Figures 2-2 through 2-9. Figures 2-2 through 2-9 simulate actual DoD operationally deployed network to strategic core network test configuration strings. The SUT was tested with other DSCD devices between the various test points denoted in each figure.



LEGEND:

4ESS	Class 4 Electronic Switching System
ADNS	Automated Digital Network System
ASLAN	Assured Services Local Area Network
CAS	Channel Associated Signaling
CEU	Channel Encryption Unit
CS	Communication Server
DRSN	Defense Red Switch Network
DSCD	Department of Defense (DoD) Secure Communications Device
EC	Echo Canceller
EWSD	Elektronisches Wählsystem Digital
GSM	Global System for Mobile Communications
GW	Gateway
IP	Internet Protocol
K	Kilobit
Mbps	Megabits per second
MFS	Multifunction Switch
NET	Network Equipment Technologies
PRI	Primary Rate Interface
PSTN	Public Switched Telephone Network
SA	Satellite Access
STE-R	Secure Terminal Equipment-RED Switch
SUT	System Under Test
SX-12	Simulator, Data Link
T1	Digital Transmission Link Level 1 (1.544 Mbps)

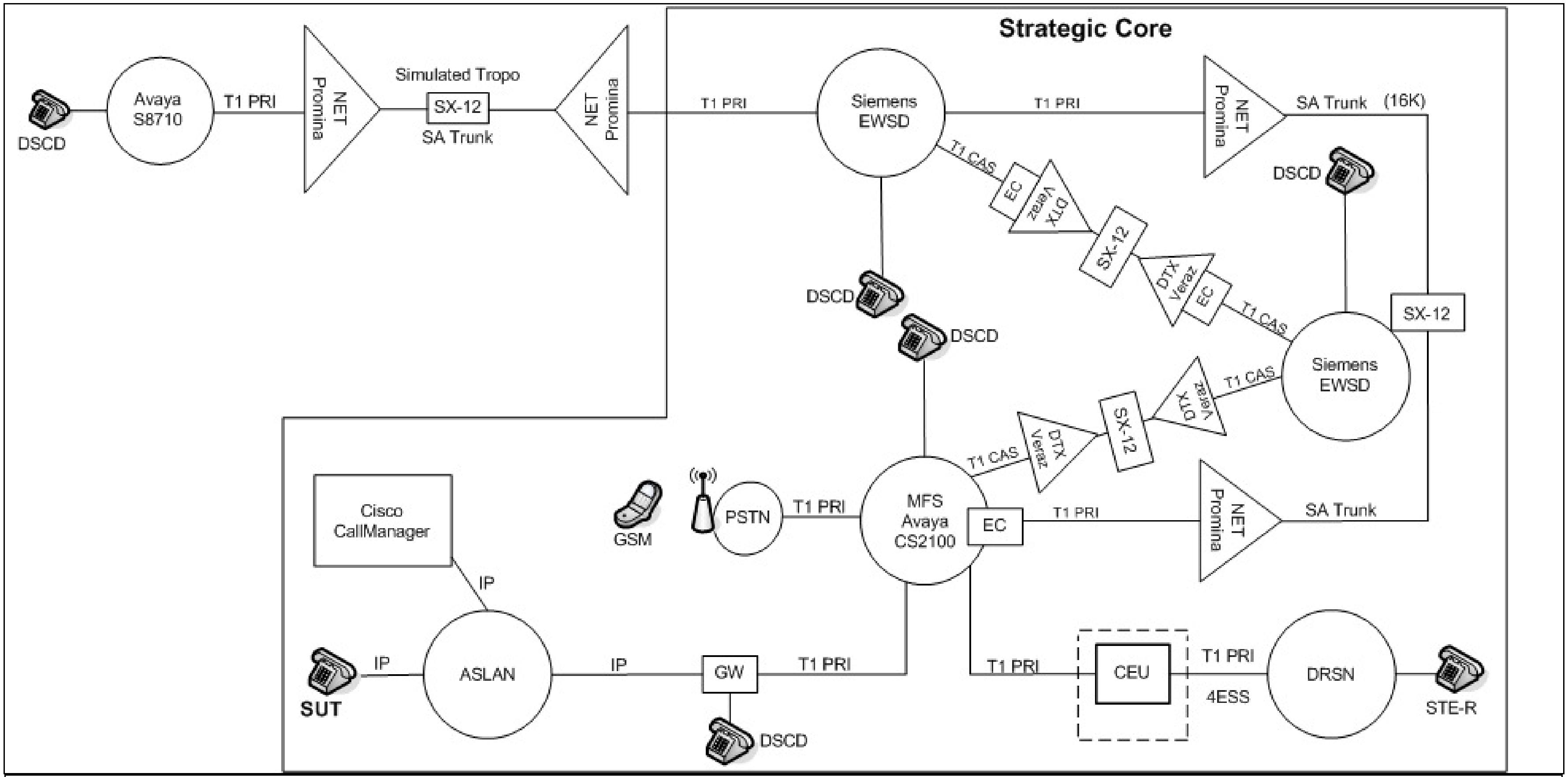
Figure 2-2. ADNS Composite Test Diagram



LEGEND:

ADNS	Automated Digital Network System
CEM	Circuit Emulation
DISN	Defense Information System Network
DSCD	Department of Defense (DoD) Secure Communications Device
EBEM	Advanced Bandwidth Efficient Modem I
EIA	Electronic Industries Alliance
EIA-530	Standard for 25-position interface for data terminal equipment and data circuit-terminating equipment employing serial binary data interchange
FXS	Foreign Exchange Station
IWF	Interworking Function
JITC	Joint Interoperability Test Command
Mbps	Megabits per second
PBX	Private Branch Exchange
PRI	Primary Rate Interface
SCIP	Secure Communication Interoperability Protocol
STE	Secure Terminal Equipment
T1	Digital Transmission Link Level 1 (1.544 Mbps)

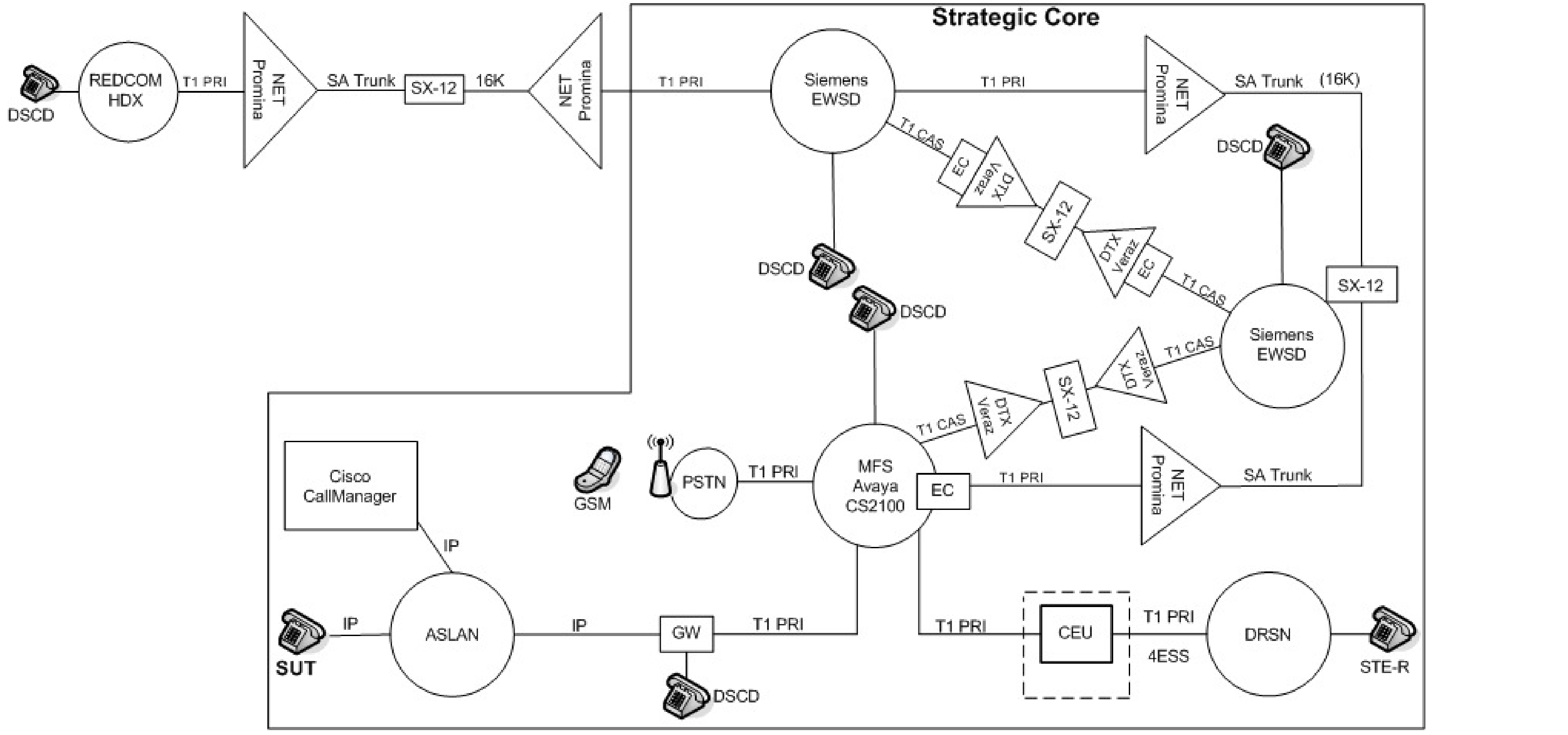
Figure 2-3. ADNS Test Network



LEGEND:

4ESS	Class 4 Electronic Switching System
ASLAN	Assured Services Local Area Network
CAS	Channel Associated Signaling
CEU	Channel Encryption Unit
CS	Communication Server
DRSN	Defense Red Switch Network
DSCD	Department of Defense (DoD) Secure Communications Device
EC	Echo Canceller
EWSD	Elektronisches Wählsystem Digital
GSM	Global System for Mobile Communications
GW	Gateway
IP	Internet Protocol
K	Kilobit
Mbps	Megabits per second
MFS	Multifunction Switch
NET	Network Equipment Technologies
PRI	Primary Rate Interface
PSTN	Public Switched Telephone Network
SA	Satellite Access
STE-R	Secure Terminal Equipment-RED Switch
SUT	System Under Test
SX-12	Simulator, Data Link
T1	Digital Transmission Link Level 1 (1.544 Mbps)
Tropo	Tropospheric Scatter Radio

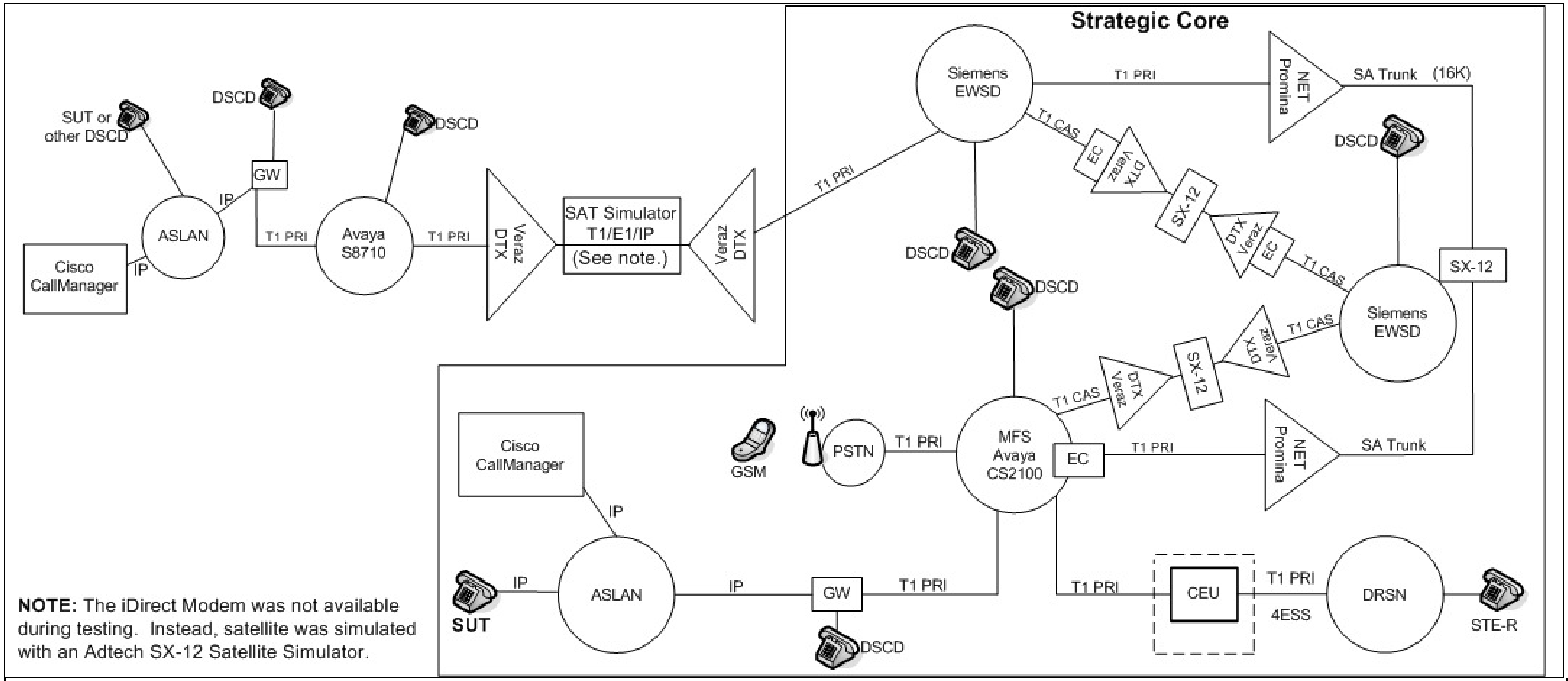
Figure 2-4. Air Force Composite Test Diagram



LEGEND:

4ESS	Class 4 Electronic Switching System	EC	Echo Canceller	NET	Network Equipment Technologies
ASLAN	Assured Services Local Area Network	EWSD	Elektronisches Wählsystem Digital	PRI	Primary Rate Interface
CAS	Channel Associated Signaling	GSM	Global System for Mobile Communications	PSTN	Public Switched Telephone Network
CENTCOM	Central Command	GW	Gateway	SA	Satellite Access
CEU	Channel Encryption Unit	HDX	High Density Exchange	STE-R	Secure Terminal Equipment-RED Switch
CS	Communication Server	IP	Internet Protocol	SUT	System Under Test
DRSN	Defense Red Switch Network	K	Kilobit	SX-12	Simulator, Data Link
DSCD	Department of Defense (DoD) Secure Communications Device	Mbps	Megabits per second	T1	Digital Transmission Link Level 1 (1.544 Mbps)
		MFS	Multifunction Switch		

Figure 2-5. CENTCOM Dual Hop Composite Test Diagram

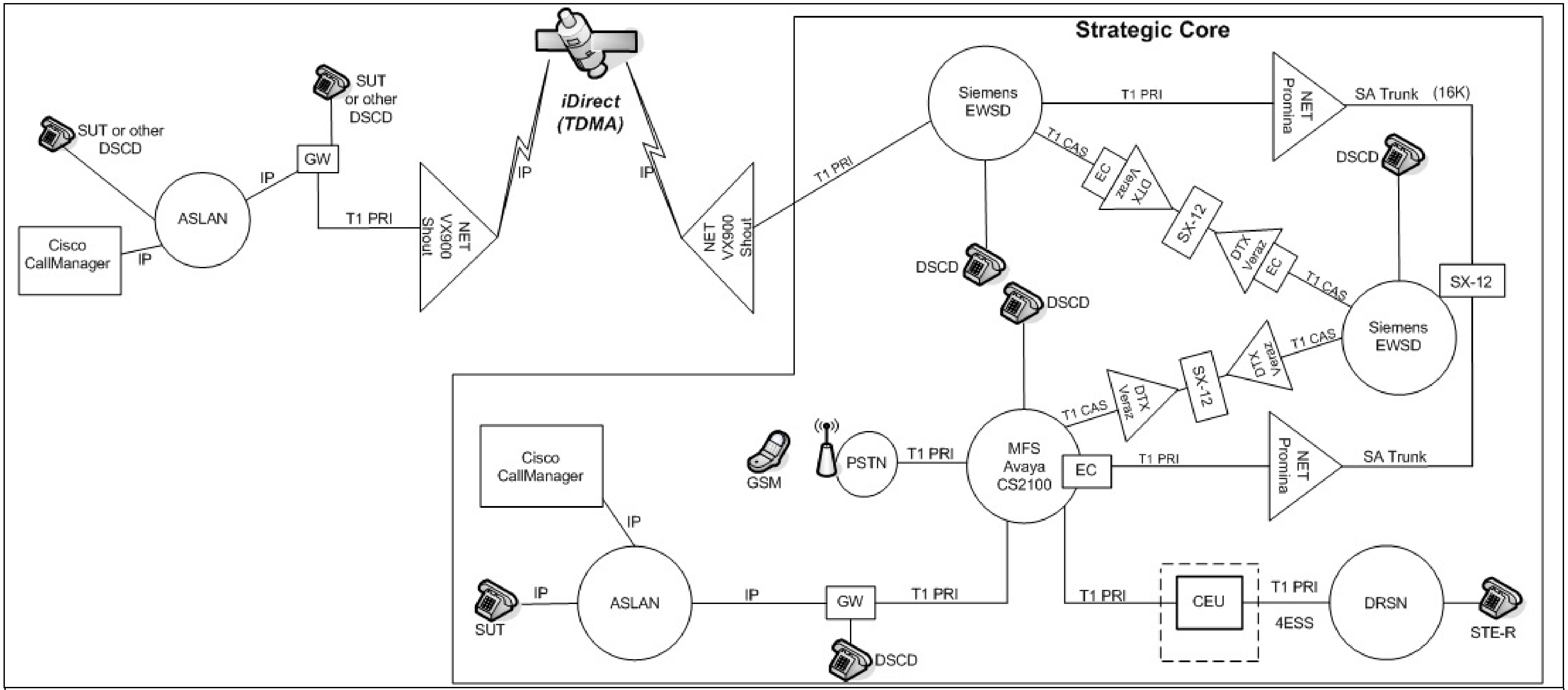


NOTE: The iDirect Modem was not available during testing. Instead, satellite was simulated with an Adtech SX-12 Satellite Simulator.

LEGEND:

4ESS	Class 4 Electronic Switching System	E1	European Basic Mutilplex Rate (2.048 Mbps)	NET	Network Equipment Technologies
ASLAN	Assured Services Local Area Network	EC	Echo Canceller	PRI	Primary Rate Interface
CAS	Channel Associated Signaling	EWSD	Elektronisches Wählsystem Digital	PSTN	Public Switched Telephone Network
CENTCOM	Central Command	GSM	Global System for Mobile Communications	SA	Satellite Access
CEU	Channel Encryption Unit	GW	Gateway	SAT	Subscriber Access Termination
CS	Communication Server	IP	Internet Protocol	STE-R	Secure Terminal Equipment-RED Switch
DRSN	Defense Red Switch Network	K	Kilobit	SUT	System Under Test
DSCD	Department of Defense (DoD) Secure Communications Device	Mbps	Megabits per second	SX-12	Simulator, Data Link
		MFS	Multifunction Switch	T1	Digital Transmission Link Level 1 (1.544 Mbps)

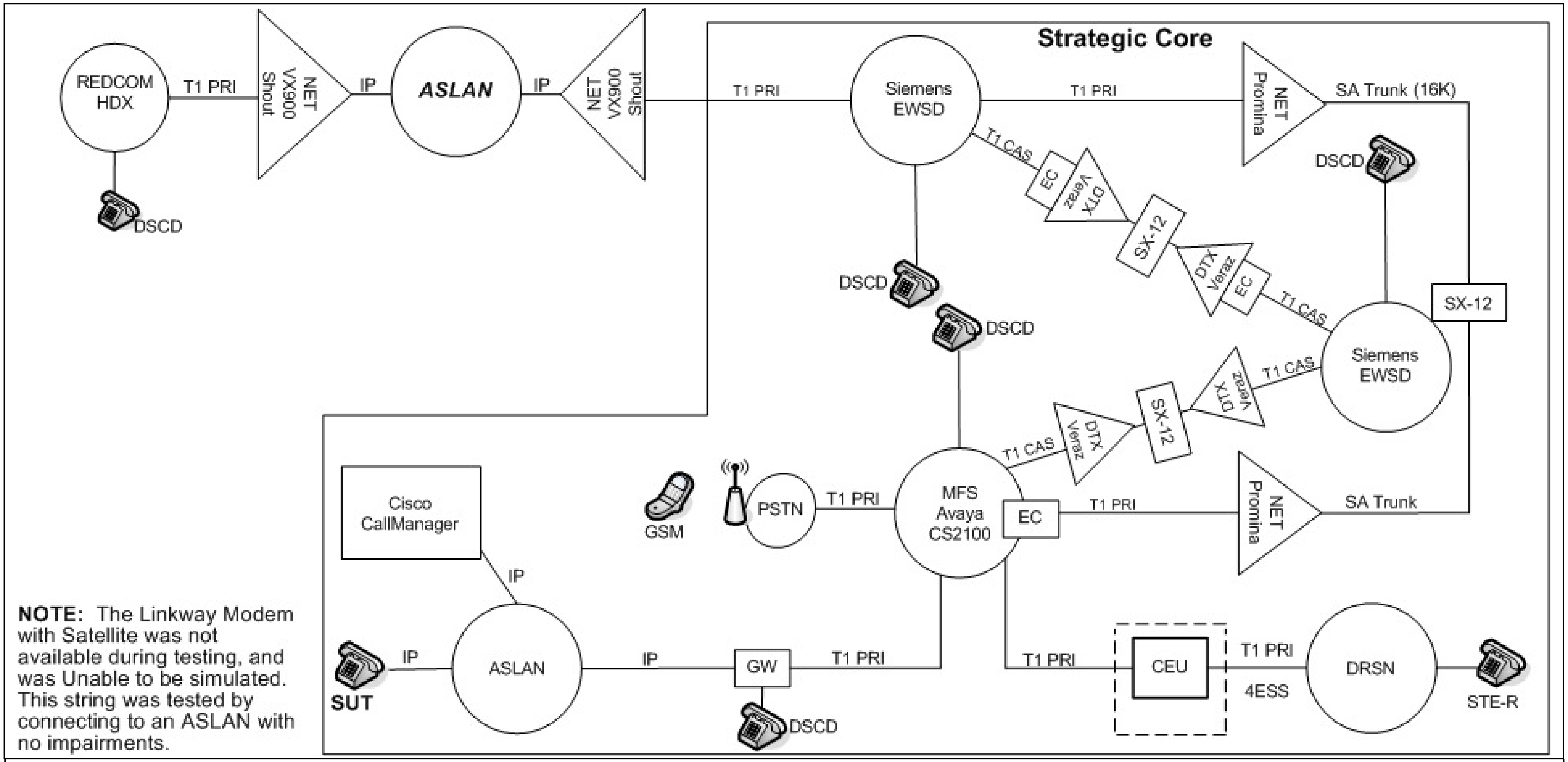
Figure 2-6. CENTCOM Composite Test Diagram



LEGEND:

4ESS	Class 4 Electronic Switching System
ASLAN	Assured Services Local Area Network
CAS	Channel Associated Signaling
CEU	Channel Encryption Unit
CS	Communication Server
DRSN	Defense Red Switch Network
DSCD	Department of Defense (DoD) Secure Communications Device
EC	Echo Canceller
EWSD	Elektronisches Wählsystem Digital
GSM	Global System for Mobile Communications
GW	Gateway
IP	Internet Protocol
JCSE	Joint Communications Support Element
K	Kilobit
Mbps	Megabits per second
MFS	Multifunction Switch
NET	Network Equipment Technologies
PRI	Primary Rate Interface
PSTN	Public Switched Telephone Network
SA	Satellite Access
STE-R	Secure Terminal Equipment-RED Switch
SUT	System Under Test
SX-12	Simulator, Data Link
T1	Digital Transmission Link Level 1 (1.544 Mbps)
TDMA	Time Division Multiple Access

Figure 2-7. JCSE DSCD Composite Test Diagram

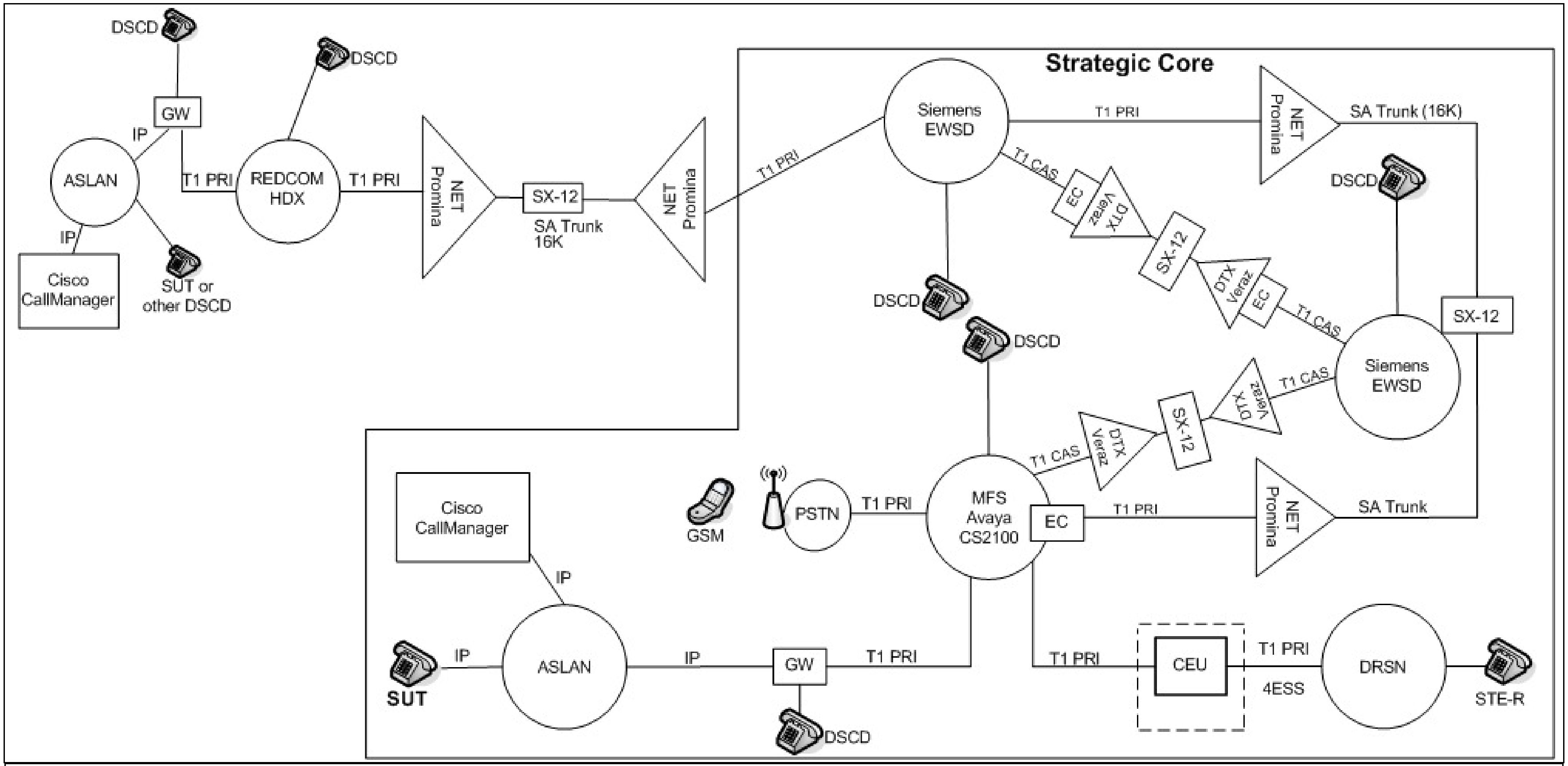


NOTE: The Linkway Modem with Satellite was not available during testing, and was Unable to be simulated. This string was tested by connecting to an ASLAN with no impairments.

LEGEND:

4ESS	Class 4 Electronic Switching System
ASLAN	Assured Services Local Area Network
CAS	Channel Associated Signaling
CEU	Channel Encryption Unit
CS	Communication Server
DRSN	Defense Red Switch Network
DSCD	Department of Defense (DoD) Secure Communications Device
EC	Echo Canceller
EWSD	Elektronisches Wählsystem Digital
GSM	Global System for Mobile Communications
GW	Gateway
HDX	High Density Exchange
IP	Internet Protocol
K	Kilobit
Mbps	Megabits per second
MFS	Multifunction Switch
NET	Network Equipment Technologies
PRI	Primary Rate Interface
PSTN	Public Switched Telephone Network
SA	Satellite Access
STE-R	Secure Terminal Equipment-RED Switch
SUT	System Under Test
SX-12	Simulator, Data Link
T1	Digital Transmission Link Level 1 (1.544 Mbps)
USMC	United States Marine Corps

Figure 2-8. USMC Composite Test Diagram



LEGEND:

4ESS	Class 4 Electronic Switching System
ASLAN	Assured Services Local Area Network
CAS	Channel Associated Signaling
CEU	Channel Encryption Unit
CS	Communication Server
DRSN	Defense Red Switch Network
DSCD	Department of Defense (DoD) Secure Communications Device
EC	Echo Canceller
EWSD	Elektronisches Wählsystem Digital
GSM	Global System for Mobile Communications
GW	Gateway
HDX	High Density Exchange
IP	Internet Protocol
K	Kilobit
Mbps	Megabits per second
MFS	Multifunction Switch
NET	Network Equipment Technologies
PRI	Primary Rate Interface
PSTN	Public Switched Telephone Network
SA	Satellite Access
STE-R	Secure Terminal Equipment-RED Switch
SUT	System Under Test
SX-12	Simulator, Data Link
T1	Digital Transmission Link Level 1 (1.544 Mbps)
WIN-T	Warfighter Information Network - Tactical

Figure 2-9. WIN-T Composite Test Diagram

9. SYSTEM CONFIGURATIONS. Table 2-3 provides the system configurations, hardware, and software components tested with the SUT. The SUT was tested in an operationally realistic environment as depicted in Figures 2-2 through 2-9 to determine interoperability with other DSCD end instruments also listed in Table 2-3. The SUT is certified with any CCM solution on the UC APL with the following limitation: the CCM solution must be configured with 2800, 3700, or 3800 series gateways that are loaded with IOS versions 12.4(22)T2 or later for the 2800 series gateways and IOS 12.4(15) T8 or later for the 3700 and 3800 series gateways. The SUT is also certified with the CUCM with software version 7.1(2) on the UC APL.

Table 2-3. Tested System Configurations

System Name		Software Release	
Avaya CS2100		Succession Enterprise (SE) 09.1	
Nokia-Siemens EWSD		19d with Patch Set 46	
Avaya S8710		Communication Manager (CM) 4.0 (R014x.00.2.731.7: Super Patch 14419)	
Cisco CallManager		4.3(2) Service Release (SR) 1b with IOS Software Release 12.4(15) T8	
Cisco Unified Communications Manager		7.1(2) with IOS Software Release 12.4(22)T2	
REDCOM High Density Exchange		Release 3.0A Revision 3, with Specified Patch Group 0 (3.0A R3P0)	
Raytheon Channel Encryption Unit (CEU)		Release Version (v) 2.01.08 with LogiTel Mesh Router (MR) 1060 Release Version (v) 1.01.0205	
L3 Communications STE and STE-R		2.6 and 2.7 with KSV-21	
L3 Communications Omni Secure Wireline Terminal		5.07	
L3 Communications Omni Secure Wireline Terminal		6.01	
General Dynamics Sectéra® Wireline Terminal		12.05	
General Dynamics IP vIPer (Model SVT1000SM)		1.0 Version 6.04	
General Dynamics PSTN vIPer (Part Numbers VIPS1000XA and VIPS1000XA)		2.14	
NET Promina 800 and 400		4.x.2.02 Version 92.45	
NET VX900		4.3.5 Version 55	
Veraz DTX 600		JITC022.1	
SUT	L-3 Communications IP STE Release 1.2.4	Boot Processor	0023
		Audio Controller	P1
		Host Processor	0615
		Network Processor	V173
		10/100 Base Ethernet Card	NA

LEGEND:

CS	Communication Server	NA	Not Applicable
EWSD	Elektronisches Wählsystem Digital	PBX 1	Private Branch Exchange 1
IOS	Internetwork Operating System	PSTN	Public Switched Telephone Network
IP	Internet Protocol	SMEO	Small End Office
JITC	Joint Interoperability Test Command	STE	Secure Terminal Equipment
MFS	Multifunction Switch	STE-R	Secure Terminal Equipment-RED Switch
NET	Network Equipment Technologies	SUT	System Under Test

10. TESTING LIMITATIONS. None.

11. TEST RESULTS

a. Discussion.

(1) The UCR, 2008 Change 1 section 5.2.5.2, states that DSCD shall be only those that are Type Approved by the NSA and are listed on the NSA Secure Product Web site. Each DSCD must support at least one NSA approved secure protocol. If the DSCD supports more than one secure protocol, it must meet all the requirements for at least one of the secure protocols, and must minimally support the other protocols that are provided on the DSCD. The SUT received an NSA Type I accreditation for all protocols supported (SCIP and STE mode) on 12 October 2010, which meets this requirement.

(2) The UCR, 2008 Change 1 section 5.2.5.2, states that DSCDs that establish secure sessions on IP networks using SCIP shall satisfy all of the end point requirements described in UCR 2008, Change 1, Section 5.3.2 Assured Services Requirements, SCIP-215, and SCIP-216. This requirement was met with vendor submission of an LoC.

(3) The UCR, section 5.2.5.2, states that DSCD devices that use an IP interface shall meet the end instrument requirements as specified in UCR 2008, Change 1, Section 5.3.2 Assured Services Requirements. The SUT met the requirements in accordance with UCR 2008, Change 1, Section 5.3.2 Assured Services Requirements as described below:

(a) The UCR, section 5.2.12.8.2.7, states the VoIP systems shall not be greater than 60 milliseconds (ms) averaged over any five-minute period. The latency is to be measured from IP handset to egress from the VoIP system via a DSN trunk. The SUT had a measured one-way latency of 65 ms from handset to the Digital Transmission Link Level 1 (T1) Integrated Services Digital Network (ISDN) Primary Rate Interface (PRI) gateway trunk egress, which did not meet this requirement. This discrepancy was adjudicated by DISA and the Theater Joint Tactical Network (TJTN) as having a minor operational impact.

(b) The UCR, section 5.2.12.8.2.8, states that the VoIP systems (a combination of call control and End Instruments) must meet Internet Protocol Version 6 (IPv6) capability requirements as defined in UCR 2008, Section 5.3.5. The SUT does not support IPv6. The Office of the Secretary of Defense waived the IPv6 requirements on 27 September 2010 with the stipulation that the vendor provide a commitment to upgrade to IPv6 and demonstrate it during the Spiral 2 IPv6 Pilot test starting in the summer of 2011.

(c) The UCR, section 5.2.12.8.2.9, states that the VoIP system shall meet the service class tagging requirements as provided in UCR 2008, Section 5.3.1. In accordance with this reference, the SUT is required to tag layer 3 Internet Protocol version 4 (IPv4) IP traffic with a Differentiated Services Code Point (DSCP) tag any value 0 through 63 distinctively for voice media and voice signaling. The SUT however does not have the ability to set DSCP voice media and voice signaling distinctively any value 0 to 63. The SUT is hard coded with DSCP values of 0 for signaling and 40 for media. This discrepancy was adjudicated by DISA and the TJTN as having a minor operational impact with a Plan of Action and Milestones (POAM). The vendor stated in their POAM that this capability will be added in the next release of the SCCP IP STE in late 2011.

(4) The UCR, section 5.2.5.2, states that a DSCD device that supports one of the required signaling modes shall interoperate with and establish secure session with other compatible devices with at least a 85 percent secure call completion rate. A total of approximately 4700 secure calls were placed with the SUT to other DSCD secure devices listed in Table 2-2 over the test configurations depicted in Figures 2-2 through 2-9 with a secure call completion rate of 90 percent or better, which meets this requirement. All calls that were placed established a secure call, and then were manually placed non-secure, then placed in secure mode again without initiating a new non-secure call for a series of ten calls in each direction over each test string.

(5) The UCR, section 5.2.5.2, states that the DSCD shall be capable of using the protocols provided to establish a secure session within 60 seconds and must maintain secure communications for the duration of the secure portion of the call. The SUT setup secure calls over the test configurations depicted in Figures 2-2 through 2-9. All calls established a secure connection within 42 seconds and maintained calls until sessions were ended, when placing calls to other DSCD devices that have ISDN or Analog interfaces. When placing calls to other IP DSCD devices that support the Modem V.150.1 standard, secure calls will establish within 10 seconds, which meets this requirement.

(6) The UCR, section 5.2.5.2, states that the DSCD shall operate in a network that has an end-to-end latency of up to 600 ms. The SUT was able to establish secure calls over the test configurations depicted in Figures 2-2 through 2-9. The maximum end-to-end latency was 1100 ms before the SUT was unable to establish secure communications which meets the requirement.

(7) The UCR, section 5.2.5.2, states that the DSCD shall achieve and maintain a secure voice connection with a minimum Mean Opinion Score (MOS) of 3.0. A SAGE 960B was used to measure SMOS from the handset of the SUT. The SUT secure voice connection at 9.6 kilobits per second (kbps) Conjugate-Structure Algebraic-Code-Excited Linear-Prediction (CS-A CELP) measured a MOS from 3.7 to 4.07 for an average of 3.85, which meets this requirement.

(8) The UCR, section 5.2.5.2, states that once connected to the rekey center, the DSCD shall obtain a new key and properly process that new key with a 95 percent rekey completion rate. The SUT rekey completion rate over test configurations depicted in Figures 2-2 through 2-9 was 100 percent for all rekey calls attempted, which meets this requirement.

(9) The UCR, section 5.2.5.2, states that DSCD devices shall support a minimum data rate and facsimile (fax) transmission rate of 9.6 kbps. A total of approximately 50 secure data calls were placed over the test diagrams depicted in

Figures 2-2 through 2-9 with the SUT via the SUT's serial interface. All calls were successful with a data rate of 9.6 kbps, which meets this requirement. All asynchronous transmissions used for secure faxes with an asynchronous fax machines completed with a rate of 100 percent. In addition, all Data Transfer Device key transfer attempts and all asynchronous data BERT attempts were successful and were within the requirements.

b. Test Summary. The SUT met all of the critical interoperability requirements for a DSCD and is certified for joint use within the Defense Information System Network (DISN) with any Cisco CCM solution on the UC APL or CUCM with software version 7.1(2) with the following limitation: the CCM solution must be configured with 2800, 3700, or 3800 series gateways that are loaded with IOS versions 12.4(22)T2 or later for the 2800 series gateways and IOS 12.4(15) T8 or later for the 3700 and 3800 series gateways.

12. TEST AND ANALYSIS REPORT. No detailed test report was developed in accordance with the Program Manager's request. JITC distributes interoperability information via the JITC Electronic Report Distribution (ERD) system, which uses Unclassified-But-Sensitive Internet Protocol Router Network (NIPRNet) e-mail. More comprehensive interoperability status information is available via the JITC System Tracking Program (STP). The STP is accessible by .mil/gov users on the NIPRNet at https://stp.fhu.disa.mil. Test reports, lessons learned, and related testing documents and references are on the JITC Joint Interoperability Tool (JIT) at http://jit.fhu.disa.mil (NIPRNet), or http://199.208.204.125 (SIPRNet). Information related to DSN testing is on the Telecom Switched Services Interoperability (TSSI) website at http://jitc.fhu.disa.mil/tssi. Due to the sensitivity of the information, the Information Assurance Accreditation Package (IAAP) that contains the approved configuration and deployment guide must be requested directly through government civilian or uniformed military personnel from the Unified Capabilities Certification Office (UCCO), e-mail: ucco@disa.mil.